Guest Editorial: Security and Privacy Issues in Industry 4.0 Applications

IN 2011, a group of delegates from business and academia, and politics in German initially proposed the conception of the Fourth Industrial Revolution (or Industry 4.0), which aims to improve the competitive ability in the manufacturing industry of their country. Along with the emergence of the Industry 4.0 term, people started introspecting the existing shortcomings in contemporary industrial society. Especially, the technologies of the past generations cannot maintain data explosive requirements in the Internet and telecommunication industry and fuse real-time data, which would increase waste and reduce productivity and overall equipment effectiveness.

Industry 4.0 recognizes the importance of this issue and makes full use of large-scale machine-to-machine communication and the Internet of things (IoT) to increase automation, improve communication, and self-monitoring and diagnose issues without human intervention, finally transforming traditional manufacturing and industrial practices into a modern smart organization. However, with the rapid growth of devices, security and privacy issues rise to the surface. A mass amount of data frequently exchanged in the public channel will draw the attention of some people with evil intentions. Moreover, the resource-limited devices without strong cryptographic assurance would be compromised and hacked by adversaries. Hence, assuring the authenticity, integrity, and nonrepudiation of these industrial IoT data is a hot issue for industry 4.0 at present.

In this special issue, we have received cutting-edge technologies and novel studies, which can promote the effectiveness and advantages of advancing industrial 4.0. The response to our call for this special issue was overwhelming. During the review process, each article was assigned to and reviewed by at least three experts in the field, with a rigorous multiround review process. The designated 19 high-quality articles cover a wide range of the special issue.

The data generated in the Industrial Internet of Things (IIoT) is very sensitive and hence the privacy and security of this data are of significant importance. Sanwar Hosen *et al.* [A1] proposed a novel framework for storing, sharing, and computing the IIoT data in a secured manner. The proposed framework used a lightweight encryption method integrated with ElGamal digital signature and encryption method for ensuring the privacy and security of IIoT data.

Gao *et al.* [A2] proposed a novel federated learning-based approach to defend Industry 4.0 applications from malicious uploads. The authors have also used cryptography solutions for preventing privacy attacks on the server-side. The secure partial aggregation scheme designed by the authors improves the robustness and privacy preservation of federated learning.

Dohare *et al.* [A3] proposed a novel approach to ensure security in an industrial network. In this article, the industrial data are collected by the data owners from several resource-constrained devices that are then sent to the data aggregator. The proposed proficient CLASS ensures that the data aggregation is more secured when compared to the existing approaches. The proposed approach includes public viability, mutual authentication, confidentiality, and integrity of the data, and preserves the privacy of the industrial data.

The sensing and actuating devices in IIoT generate huge volumes of data that raise serious scalability, privacy, and security concerns. To address these challenges in IIoT, Kumar *et al.* [A4] proposed a privacy-preserved threat intelligence framework (P2TIF). The proposed framework is designed to identify cyber threats and preserve confidential and sensitive data in IIoT. The proposed framework employs a blockchain-based solution to ensure secured communication of the IIoT data and also to present data poisoning attacks. The proposed framework also employs a deep learning-based approach, namely, a deep variational autoencoder for transforming the actual data into another format to protect the data from inference attacks. Later, an attention-based deep gated recurrent neural network is employed to identify the malicious patterns in the data.

Xu *et al.* [A5] proposed a solution for secure the IIoT data transmitted through 5G. A secured cross-layer authentication framework that is inspired by quantum walk on circles is proposed in this article to secure the IIoT data. In this article, random hash encoring is performed by the proposed system on multidomain physical-layer resources for encoding and decoding the device identifiers in a secured manner, while preserving privacy. The proposed approach derives the upper bound of decoding errors and formulates the minimization of nonconvex integer programming problems to improve the security.

In the development of mobile apps, reading confidential and private information is often necessary, which may lead to the leakage of private and sensitive data of the enterprises. To address this issue, Gong *et al.* [A6] proposed a novel web APIs recommendation scheme that employs locality sensitive hashing mechanism to recommend web APIs to the developers, while preserving the privacy of the enterprise data.

Date of current version June 13, 2022.
Digital Object Identifier 10.1109/TII.2022.3164741

Federated learning is envisioned as a promising solution to ensure the privacy of the sensitive data generated from IIoT applications. However, the malicious participants can train the local model on poisoning samples and hence jeopardize the functioning of the global model. To address this issue, Zhang *et al.* [A7] proposed a novel RobustFL method for defending the IIoT attacks from poisoning attacks. In this article, an adversarial training framework is conducted, where a predictive model based on extra logits is built at the server for predicting which participant owns a given logit. Based on these predictions, the federated learning model is trained adversary to prevent which prevents the predictive behavior, thereby mitigating the influences of poisonous attacks.

Tahir *et al.* [A8] proposed a novel approach to tackle false data injection attacks (FDIA) in Industry 4.0 applications. To prevent data breaches by FDIA, a recurrent deep deterministic policy gradient is employed to invent an experience-driven FDIA in the IoT-based transactive energy systems. A deep federated learning-based decentralized FDIA detection scheme is used in this article to prevent attackers exploiting the data integrity in smart energy meters. The proposed approach can achieve parallel computing and identify the stealthy FDIA on several nodes simultaneously.

The growing numbers of IIOT-based applications that generate a huge amount of sensitive and confidential data have resulted in numerous cyber-attacks. To address this issue, Makkar *et al.* [A9] proposed a safe data sharing architecture for IIoT devices through federated learning. The federated learning is employed in the consensus process of edge computing, thereby leading to high efficiency, enhances privacy preservation, and security.

Qahtan *et al.* [A10] formulated a novel fuzzy weighted with zero inconsistency for weighing the privacy and security properties for benchmarking blockchain-based healthcare systems. A decision matrix was formulated in the first phase based on the intersection of security and privacy properties such as access control, user authentication, integrity, and blockchain-based IoT healthcare Industry 4.0 systems. Later, the weights of each privacy and security property are calculated through the proposed method. The resulting weights are used to benchmark blockchain-based healthcare systems using a combined grey relational analysis technique for order of preference by bald eagle search optimization method and similarity to an ideal solution.

As the sensors in IIoT applications collect crucial social life and production-related information, designing an efficient and secured communication challenge is a key research challenge. To address this issue, Fan *et al.* [A11] proposed a novel authentication and key exchange protocol named SAKE* that employs two types of keys, evolution and master keys, to guarantee perfect forward security for IIoT devices. To achieve integrity of the messages, key exchange, and lightweight authentication, the SAKE* employs hash function, XOR, and concatenation operations.

Cybercriminals are often targeting IIoT applications due to the sensitive and crucial data generated from them. In this context, flexible, fast, and lightweight security solutions are the need of the hour to solve the security-related issues in IIoT applications. To this effect, Latif *et al.* [A12] proposed a lightweight dense random neural network to detect intrusions in IoT devices. Due to its inherent distributed and improved generalization capabilities, the proposed scheme is well suited for the resource- constrained IoT devices. The proposed scheme was evaluated on a popular IoT security dataset, ToN_IoT.

Anajemba *et al.* [A13] proposed an efficient privacy-preserving protocol to guard against eavesdropping attacks in IIoT applications. The authors have formulated a closed-form derivation for an asymptotic regularized prompt privacy rate to achieve this for IIoT devices. Later, optimal jamming parameters are designed through an optimal counter-eavesdropping channel approximation model for handling eavesdropping attacks in IIoT devices.

Kautish *et al.* [A14] proposed a novel distributed denial-of-service mitigation strategy in a hybrid cloud environment that employs a scattered denial-of-service mitigation tree architecture. An integrated network monitoring is used in the proposed framework for enabling detection procedures.

Teimoori *et al.* [A15] proposed a secured cloudlet-based recommendation system for electric vehicles to ensure privacy preservation. The proposed model employs a vertical federated learning technique for PNG privacy preservation in electric vehicles. The cloudlet-based data aggregators are used in the proposed approach to address communication concerns and to improve the efficiency of the model. Blockchain technology, which is responsible for generating a trusted cloudlet networks, is used to enhance the security of the proposed system.

The load forecasting in the power grid directly affects the economy of the supply demand balance, the rationality of the grid planning, and the safety of the grid operation. However, the forecasting of the load is made complicated by several factors that may lead to drastic changes in short-term power consumption. To address this problem, "Lv *et al.* [A16] proposed a novel hybrid model based on long short-term memory and variational mode decomposition with seasonal factors estimation and error correction. To demonstrate the practicality and effectiveness of the proposed hybrid model, four real-world data sets from the United States and Singapore are employed in this article.

Sun *et al.* [A17] proposed a secured and privacy-preserving bilateral access control scheme with fine granularity to address the issues of privacy and security of healthcare application of IIoT. The proposed scheme employs matching encryption technologies and fine-grained access control to ensure that both healthcare providers and patients can specify their fine-grained access control on the encrypted health related data, so that only the authorized personnel can access the sensitive healthcare data.

Velliangiri *et al.* [A18] proposed a flexible and lightweight authentication method for secured in-vehicle data exchange. XOR operations, lightweight operations, and concatenation are used in the proposed protocol. AVISPA is used to evaluate the security of the proposed approach.

Qi *et al.* [A19] proposed a novel anomaly detection mechanism, namely MSD_AD to tackle the dynamic nature of the intrusion detection data in the logistics network on Industry 4.0. The proposed scheme employs PCA, isolation forest, and locality sensitive hashing techniques. The locality-sensitive hashing

can handle multiaspect data, MSD_AD can detect group analysis from experimental results, whereas PCA is used to reduce the dimensionality for correlations between several attributes.

Acknowledgment

The Guest Editors would like to thank all the authors who submitted their high-quality works and also the reviewers for their critical comments that contributed to improving the quality of the submitted articles that were finally accepted for publication. The Guest Editors would like to thank Prof. R. Luo, Editor-in-Chief, TII, for his continuous support and guidance in preparing and finalizing this special session. The Guest Editors would also like to thank the TII staff for the professional support provided.

Mamoun Alazab, *Guest Editor*
College of Engineering, IT and Environment
Charles Darwin University
Casuarina, NT 0810, Australia

Thippa Reddy Gadekallu, *Guest Editor*
School of Information Technology and Engineering
Vellore Institute of Technology
Vellore, Tamil Nadu 632014, India

Chunhua Su, *Guest Editor*
Division of Computer Science
University of Aizu
Aizuwakamatsu 965-8580, Japan

Appendix: Related Articles

[A1] A. S. M. Sanwar Hosen *et al.,* "SPTM-EC: A security and privacy-preserving task management in edge computing for IIoT," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3123260.

[A2] J. Gao *et al.*, "Secure partial aggregation: Making federated learning more robust for industry 4.0 applications," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2022.3145837.

[A3] I. Dohare *et al.*, "Certificateless aggregated signcryption scheme (CLASS) for cloud-fog centric industry 4.0," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2022.3142306.

[A4] P. Kumar *et al.*, "P2TIF: A blockchain and deep learning framework for privacy-preserved threat intelligence in industrial IoT," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2022.3142030.

[A5] D. Xu *et al.*, "Cross-layer device authentication with quantum encryption for 5G enabled IIoT in industry 4.0," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3130163.

[A6] W. Gong *et al.*, "Efficient web APIs recommendation with privacy-preservation for mobile app development in Industry 4.0," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3133614.

[A7] J. Zhang *et al.*, "RobustFL: Robust federated learning against poisoning attacks in industrial IoT systems," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3132954.

[A8] B. Tahir *et al.*, "Experience driven attack design and federated learning based intrusion detection in industry 4.0," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3133384.

[A9] A. Makkar *et al.*, "SecureIIoT environment: Federated learning empowered approach for securing IIoT from data breach," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2022.3149902.

[A10] S. Qahtan *et al.*, "Novel multi security and privacy benchmarking framework for blockchain-based IoT healthcare industry 4.0 systems," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2022.3143619.

[A11] Q. Fan *et al.*, "SAKE*: A symmetric authenticated key exchange protocol with perfect forward secrecy for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2022.3145584.

[A12] S. Latif *et al.*, "Intrusion detection framework for the Internet of Things uses a dense random neural network," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3130248.

[A13] J. H. Anajemba *et al.*, "A counter-eavesdropping technique for optimized privacy of wireless industrial IoT communications," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3140109.

[A14] S. Kaushik *et al.*, "SDMTA: Attack detection and mitigation mechanism for DDoS vulnerabilities in hybrid cloud environment," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2022.3146290.

[A15] Z. Teimoori *et al.*, "A secure cloudlet-based charging station recommendation for electric vehicles empowered by federated learning," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2022.3148997.

[A16] L. Lv *et al.*, "A VMD and LSTM-based hybrid model of load forecasting for power grid security," *IEEE IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3130237.

[A17] J. Sun *et al.*, "Privacy-preserving bilateral fine-grained access control for cloud-enabled industrial IoT healthcare," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3133345.

[A18] S. Velliangiri *et al.*, "An efficient lightweight privacy-preserving mechanism for industry 4.0 based on elliptic curve cryptography," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3139609.

[A19] L. Qi *et al.*, "Fast anomaly identification based on multi-aspect data streams for intelligent intrusion detection toward secure industry 4.0," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3139363.

Mamoun Alazab (Senior Member, IEEE) received the Ph.D. degree in cyber security from the School of Science, Information Technology and Engineering, Federation University of Australia, Ballarat, VIC, Australia, in 2012.

He is currently an Associate Professor with the College of Engineering, IT and Environment, Charles Darwin University, Casuarina, NT, Australia. He is a cyber-security researcher and practitioner with industry and academic experience. His research is multidisciplinary that focuses on cyber-security and digital forensics of computer systems with a focus on cybercrime detection and prevention. He has more than 150 research papers in many international journals and conferences, such as the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, IEEE TRANSACTIONS ON BIG DATA, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, Computers & Security, and Future Generation Computing Systems.

Dr. Alazab delivered many invited and keynote speeches, 24 events in 2019 alone. He convened and chaired more than 50 conferences and workshops. He works closely with government and industry on many projects, including Northern Territory (NT) Department of Information and Corporate Services, IBM, Trend Micro, the Australian Federal Police, the Australian Communications and Media Authority, Westpac, United Nations Office on Drugs and Crime, and the Attorney General's Department. He is the Founding chair of the IEEE NT Subsection.

Thippa Reddy Gadekallu (Senior Member, IEEE) received the bachelor's degree in computer science and engineering from Nagarjuna University, Guntur, India, in 2003, the master's degree in computer science and engineering from Anna University, Chennai, India, in 2011, and the Ph.D. degree in machine learning from the Vellore Institute of Technology, Vellore, India, in 2017.

He is currently working as an Associate Professor with the School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India. He has more than 14 years of experience in teaching. He has more than 100 international/national publications in reputed journals and conferences. His research interests include machine learning, Internet of Things, deep neural networks, blockchain, and computer vision.

Dr. Gadekallu is an Editor for several publishers like Springer, Hindawi, Plosone, Scientific Reports (Nature), Wiley. He also acted as a Guest Editor for several reputed publishers like IEEE, Springer, Hindawi, MDPI. He was recently recognized as one among the top 2% scientists in the world as per the survey conducted by Elsevier in the year 2021.

Chunhua Su received the B.Sc. degree in computer science from the Beijing Electronic Science and Technology Institute, Beijing, China, in 2003, and the M.S. and Ph.D. degrees in computer science from the Faculty of Engineering, Kyushu University, Fukuoka, Japan, in 2006 and 2009, respectively.

He is currently working as a Senior Associate Professor with the Division of Computer Science, University of Aizu, Aizuwakamatsu, Japan. He worked as a Postdoctoral Fellow with Singapore Management University from 2009 to 2011 and a Research Scientist with Cryptography and Security Department of the Institute for Infocomm Research, Singapore from 2011 to 2013. From 2013 to 2016, he has worked as an Assistant professor with the School of Information Science, Japan Advanced Institute of Science and Technology, Nomi, Japan. From 2016 to 2017, he worked as an Assistant Professor with the Graduate School of Engineering, Osaka University, Suita, Japan. His research interests include cryptanalysis, cryptographic protocols, privacy-preserving technologies in machine learning and IoT security and privacy. He has authored more than 100 papers in international journals and conferences.